Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

Note: Even though a vulnerability may allow several malicious acts to be performed, only the highest level risk will be defined in the Risk column.

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium -** A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source

ALWIL Software avast! antivirus 4.6.623 and prior	A vulnerability has been reported that could let certain types of viruses go undetected. A fixed version (4.6.652) is available via the application's user interface or at: http://www.avast.com/eng/updates.html Currently we are not aware of any exploits for this vulnerability.	ALWIL avast! antivirus May Fail to Detect Certain Viruses CAN-2005-1719	Medium	Security Tracker Alert, May 18, 2005
Black Cactus Warrior Kings: Battles 1.23 & prior, Warrior Kings 1.3 & prior	Two vulnerabilities have been reported that could let remote malicious users cause a Denial of Service and potentially compromise a vulnerable system. This is due to a format string error in the text visualization and an error in the handling of partial join packets. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Black Cactus Warrior Kings Denial of Service and Format String Vulnerabilities CAN-2005-1702 CAN-2005-1703	High	Luigi Auriemma, May 23, 2005
ezdwc NewsletterEz 3.0	An input validation vulnerability has been reported that could let a remote malicious user inject SQL commands. The 'news/admin/login.asp' script does not properly validate user-supplied input in the 'password' parameter. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	exdwc NewsletterEz Input Validation Vulnerability Lets Remote Users Inject SQL Commands CAN-2005-1750	High	Secunia SA15469, May 24, 2005
Groove Workspace 2.x Groove Virtual Office 3.x	Multiple vulnerabilities have been reported that could let local malicious users view sensitive information or could let remote malicious users conduct script insertion attacks, bypass certain security restrictions, and trick users into executing malicious files. This is because files in the installation directory have improper permissions; input passed to the picture column and drop-down list of a SharePoint list is not properly validated; there is an error in the access restrictions on COM objects; and, the file extension for files attached to or embedded in a document with Microsoft Windows OLE is not properly displayed. Groove Virtual Office: Update to version 3.1a build 2364 or 3.1 build 2338: http://www.groove.net/index.cfm/pagename/UpdateGroove/ Groove Workspace: Update to version 2.5n build 1871: http://www.groove.net/index.cfm?pagename=DownloadsArchive There is no exploit code required.	Groove Virtual Office / Workspace Multiple Vulnerabilities CAN-2005-1675 CAN-2005-1676 CAN-2005-1677 CAN-2005-1678	High	US-CERT VU#443370 US-CERT VU#372618 US-CERT VU#155610 US-CERT VU#514386 US-CERT VU#232232
Ipswitch IMail Server 8.x	Multiple vulnerabilities have been reported in IMail Server, which could let a remote malicious user gain sensitive information or cause a Denial of Service. These are due to unspecified errors in the IMAP4d32 service and Web Calendaring. Apply IMail Server 8.2 Hotfix 2:	Ipswitch IMail Server Multiple Vulnerabilities	Medium	Ipswitch Support Advisory, IMail Server 8.2 Hotfix 2, May 23, 2005

	ftp://ftp.ipswitch.com/Ipswitch/ Product_Support/IMail/imail82hf2.exe Currently we are not aware of any exploits for these vulnerabilities.			
LS Games War Times 1.03 and prior versions	A vulnerability has been reported that could let a remote malicious user cause a Denial of Service. A remote user can send a specially crafted 64-byte nickname value to trigger an overflow. The game server will crash when the next connection is made to the game service. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	LS Games War Times Denial of Service CAN-2005-1718	Low	Security Tracker Alert, 1013981, May 17, 2005
Microsoft Windows Media Player 9 Series, Windows Messenger 5.0, MSN Messenger 6.1, 6.2	Several vulnerabilities exist: a vulnerability exists in Media Player due to a failure to properly handle PNG files that contain excessive width or height values, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the Windows and MSN Messenger due to a failure to properly handle corrupt or malformed PNG files, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.microsoft.com/technet/ security/bulletin/MS05-009.mspx V1.1: Bulletin updated with information on the mandatory upgrade of vulnerable MSN Messenger clients in the caveat section, as well as changes to the Workarounds for PNG Processing Vulnerability in MSN Messenger. V1.2: Bulletin updated with correct file version information for Windows Messenger 5.0 update, as well as added Windows Messenger 5.1 to "Non-Affected Software" list. V2.0: The update for Windows Messenger version 4.7.0.2009 (when running on Windows XP Service Pack 1) was failing to install when distributed via SMS or AutoUpdate. An updated package corrects this behavior. V2.1: Bulletin updated to update the "Security Update Information" section for the Microsoft Windows Messenger 4.7.0.2009 (when running on Windows XP Service Pack 1) security update. **V2.2: Updated the "deployment" section of Microsoft Windows Messenger version 4.7.0.2009 for the correct command.** An exploit script has been published for MSN Messenger/Windows Messenger PNG Buffer Overflow vulnerability.	Microsoft Media Player & Windows/MSN Messenger PNG Processing CAN-2004-1244 CAN-2004-0597	High	Microsoft Security Bulletin, MS05-009, February 8, 2005 US-CERT Technical Cyber Security Alert TA05-039A US-CERT Cyber Security Alert SA05-039A US-CERT Vulnerability Note VU#259890 Security Focus, February 10, 2005 Microsoft Security Bulletin MS05-009 V1.1, February 11, 2005 Microsoft Security Bulletin, MS05-009 V1.2, February 15, 2005 Microsoft Security Bulletin, MS05-009

				V2.0, April 12, 2005 Microsoft Security Bulletin, MS05-009 V2.1, May 11, 2005 **Microsoft Security Bulletin, MS05-009 V2.2, May 11, 2005**
Microsoft Word	A buffer overflow vulnerability has been reported that could let a malicious user execute arbitrary code. This is a issue when a '.mcw' (MacWrite II/MS Word for Macintosh) file is processed. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Microsoft Word MCW File Handler Buffer Overflow Vulnerability CAN-2005-1683	High	Security Focus, Bugtraq ID 13687, May 19, 2005
Microsoft Word 2000, 2002 Works Suite 2001, 2002, 2003, and 2004 Office Word 2003	A buffer overflow vulnerability has been reported that could lead to remote execution of arbitrary code or escalation of privilege. Updates available: http://www.microsoft.com/technet/security/Bulletin/MS05-023.mspx V1.1 Bulletin updated to point to the correct Exchange 2000 Server Post-Service Pack 3 (SP3) Update Rollup and to advise on the scope and caveats of workaround "Unregister xlsasink.dll and fallback to Active Directory for distribution of route information." V1.2: Bulletin updated to add msiexec in the administrative installation in "Administrative Deployment" section for all versions. **V1.3: Bulletin updated to reflect a corrected Winword.exe file version for Word 2000.** Currently we are not aware of any exploits for this vulnerability.	Microsoft Word Remote Code Execution & Escalation of Privilege Vulnerabilities CAN-2004-0963 CAN-2005-0558	High	Microsoft Security Bulletin MS05-023, April 12, 2005 US-CERT VU#442567 US-CERT VU#752591 Microsoft Security Bulletin MS05-023 V1.1, April 14, 2005 Microsoft Security Bulletin MS05-023 V1.2, May 11, 2005 **Microsoft Security Bulletin MS05-023 V1.3, May 18, 2005**
Miranda IM 'PopUp Plus'	A buffer overflow vulnerability has been reported that could let a remote malicious user execute arbitrary code	Miranda IM PopUp Plus	High	sec.org.il Security

2.0.3.8 plugin for Miranda Instant Messenger	on the target system. The vulnerability can be exploited if the 'Use SmileyAdd Setting' application menu option is enabled. **Update available at:** **http://files.miranda-im.org/testing/popupplus.zip** A Proof of Concept exploit has been published.	Plugin Remote Code Execution Vulnerability CAN-2005-1093		Advisory, April 6, 2005 **Security Focus, 13048, May 19, 2005**
Zone Labs ZoneAlarm Antivirus 5.x ZoneAlarm Security Suite 5.x	A integer overflow vulnerability has been reported that could let remote malicious users execute arbitrary code or gain escalated privilege. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Zone Labs ZoneAlarm Vet Antivirus Engine Buffer Overflow CAN-2005-1693	High	remote.com Security Advisory, May 22, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Apple Macintosh OS X	Multiple vulnerabilities have been reported:a Denial of Service vulnerability was reported in the 'nfs_mount()' function due to insufficient input value checks; a Directory Traversal vulnerability was reported in bluetooth-enabled systems due to an input validation error, which could let a remote malicious user obtain sensitive information; a vulnerability was reported in two system calls used to search filesystem objects due to insufficient checks on directory permissions, which could let a malicious user obtain sensitive information; a vulnerability was reported in the SecurityAgent because a malicious user can bypass a locked screensaver to start background applications; and a vulnerability was reported because a remote malicious user can bypass a download warning dialog to install potentially malicious Dashboard widgets. Updates available at: http://www.apple.com/support/downloads/ Currently we are not aware of any exploits for these vulnerabilities.	Mac OS X Multiple Vulnerabilities CAN-2005-0974 CAN-2005-1333 CAN-2005-1472 CAN-2005-1473 CAN-2005-1474	Medium	Apple Security Advisory, APPLE-SA-2005-05-19, May 19, 2005

Blue Coat Systems Blue Coat Reporter 7.x	Several vulnerabilities have been reported: a vulnerability was reported due to an unspecified error, which could let a remote malicious user obtain administrative privileges; a vulnerability was reported due to an unspecified error which could let an unprivileged remote malicious user add a license; a vulnerability was reported in the 'Add User' window due to insufficient sanitization of input passed as a username, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported in the 'Licensing' page due to insufficient sanitization of input passed as a license key, which could let a remote malicious user execute arbitrary code. Update available at: http://www.bluecoat.com/support/knowledge/advisory_reporter_711_vulnerabilities.html Currently we are not aware of any exploits for these vulnerabilities.	Blue Coat Reporter Multiple Vulnerabilities CAN-2005-1708 CAN-2005-1709 CAN-2005-1710	High	Blue Coat Systems Security Advisory, May 20, 2005
bzip2 bzip2 1.0.2	A remote Denial of Service vulnerability has been reported when the application processes malformed archives. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/b/bzip2/ **Mandriva:** **http://www.mandriva.com/security/advisories** Currently we are not aware of any exploits for this vulnerability.	bzip2 Remote Denial of Service CAN-2005-1260	Low	Ubuntu Security Notice, USN-127-1, May 17, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:091, May 19, 2005**
bzip2 bzip2 1.0.2 & prior	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions of target files. **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/b/bzip2/** **Mandriva:** **http://www.mandriva.com/security/advisories** There is no exploit code required.	BZip2 File Permission Modification CAN-2005-0953	Medium	Security Focus, 12954, March 31, 2005 **Ubuntu Security Notice, USN-127-1, May 17, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:091, May 19, 2005**
Cheetah Cheetah 0.9.16 a1	A vulnerability has been reported because modules are imported from the '/tmp' directory before searching for the path from the 'PYTHONPATH' variable, which could let a malicious user obtain elevated privileges.	Cheetah Elevated Privileges CAN-2005-1632	Medium	Secunia Advisory, SA15386, May 17, 2005 **Gentoo Linux Security Advisory, GLSA**

	Upgrades available at: http://prdownloads.sourceforge.net/cheetahtemplate/Cheetah-0.9.17rc1.tar.gz?download **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-14.xml** There is no exploit code required.			**200505-14, May 19, 2005**
eSYS Information systems Gibraltar Firewall 2.2	A vulnerability has been reported when using the optional Clam AntiVirus scanning feature due to a failure to detect certain unspecified types of viruses, which could lead to a false sense of security. Update available at: ww.gibraltar.at/ There is no exploit code required.	Gibraltar Firewall Anti-Virus Detection Virus Scanning Failure CAN-2005-1711	Medium	Security Tracker Alert, 1014030, May 23, 2005
Ferry Boender PROMS 0.7-0.10	Multiple vulnerabilities have been reported: A vulnerability was reported due to insufficient validation of several user-supplied parameters before used in SQL queries, which could let a remote malicious user execute arbitrary SQL code; a Cross-Site Scripting vulnerability was reported due to insufficient validation of HTML entries in some fields, which could let a remote malicious user execute arbitrary HTML and script code and a vulnerability was reported because an unauthorized malicious user can view/modify the project member's list. Upgrades available at: http://projects.electricmonk.nl//files/PROMS/proms-0.11.tar.gz There is no exploit code required.	PROMS Input Validation Holes Permit SQL Injection and Cross-Site Scripting CAN-2005-1734 CAN-2005-1735 CAN-2005-1736 CAN-2005-1737	High	Security Tracker Alert, 1013992, May 18, 2005
FreeBSD FreeBSD 5.4 & prior	A vulnerability was reported in FreeBSD when using Hyper-Threading Technology due to a design error, which could let a malicious user obtain sensitive information and possibly elevated privileges. Patches and updates available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:09.htt.asc SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.24 **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/l/** Currently we are not aware of any exploits for	FreeBSD Hyper-Threading Technology Support Information Disclosure CAN-2005-0109	Medium	FreeBSD Security Advisory, FreeBSD-SA-05:09, May 13, 2005 SCO Security Advisory, SCOSA-2005.24, May 13, 2005 Ubuntu Security Notice, USN-131-1, May 23, 2005 US-CERT VU#911878

	this vulnerability.			
Gentoo Linux 1.x	A vulnerability was reported in the webapp-config utility because the 'fn_show_postinst()' function creates a temporary file in an unsafe manner, which could let a malicious user obtain root privileges. The vendor has released a fixed version of net-www/webapp-config (1.10-r14). A Proof of Concept exploit has been published.	Gentoo webapp-config Insecure Temporary File CAN-2005-1707	High	Security Tracker Alert, 1014027, May 22, 2005
GNOME gEdit 2.0.2, 2.2 .0, 2.10.2	A format string vulnerability has been reported when invoking the program with a filename that includes malicious format specifiers, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code. No workaround or patch available at time of publishing. An exploit has been published.	Gedit Filename Format String CAN-2005-1686	High	Securiteam, May 22, 2005
GNU gzip 1.2.4 a, 1.2.4, 1.3.3-1.3.5	A Directory Traversal vulnerability has been reported due to an input validation error when using 'gunzip' to extract a file with the '-N' flag, which could let a remote malicious user obtain sensitive information. Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/g/gzip/ Trustix: http://http.trustix.org/ pub/trustix/updates/ Gentoo: http://security.gentoo.org/ glsa/glsa-200505-05.xml IPCop: http://ipcop.org/modules.php? op=modload&name=Downloads &file=index&req=viewdownload &cid=3&orderby=dateD **Mandriva:** **http://www.mandriva.com/ security/advisories** Proof of Concept exploit has been published.	GNU GZip Directory Traversal CAN-2005-1228	Medium	Bugtraq, 396397, April 20, 2005 Ubuntu Security Notice, USN-116-1, May 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-05, May 9, 2005 Security Focus,13290, May 11, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005**
GNU gzip 1.2.4, 1.3.3	A vulnerability has been reported when an archive is extracted into a world or group writeable directory, which could let a malicious user modify file permissions. Ubuntu:	GNU GZip File Permission Modification CAN-2005-0988	Medium	Security Focus, 12996, April 5, 2005 Ubuntu Security Notice, USN-116-1, May 4,

	http://security.ubuntu.com/ ubuntu/pool/main/g/gzip/ Trustix: http://http.trustix.org/ pub/trustix/updates/ Gentoo: http://security.gentoo.org/ glsa/glsa-200505-05.xml **Mandriva: http://www.mandriva.com/ security/advisories** There is no exploit code required.			2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0018, May 6, 2005 Gentoo Linux Security Advisory, GLSA 200505-05, May 9, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005**
GNU zgrep 1.2.4	A vulnerability has been reported in 'zgrep.in' due to insufficient validation of user-supplied arguments, which could let a remote malicious user execute arbitrary commands. A patch for 'zgrep.in' is available in the following bug report: http://bugs.gentoo.org/ show_bug.cgi?id=90626 **Mandriva: http://www.mandriva.com/ security/advisories** There is no exploit code required.	Gzip Zgrep Arbitrary Command Execution CAN-2005-0758	High	Security Tracker Alert, 1013928, May 10, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:092, May 19, 2005**
Igor Khasilev Oops Proxy Server 1.4.22, 1.5.53	A format string vulnerability has been reported due to insufficient sanitization of user-supplied input before passing to a formatted printing function, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/ glsa/glsa-200505-02.xml **Debian: http://security.debian.org /pool/updates/main/o/oops/** Currently, we are not aware of any exploits for this vulnerability.	Oops! Proxy Server Remote Format String CAN-2005-1121	High	Security Focus, 13172, April 14, 2005 Gentoo Linux Security Advisory, GLSA 200505-02, May 6, 2005 **Debian Security Advisory, DSA 726-1, May 20, 2005**
Iron Bars SHell Iron Bars SHell 0.3a-0.3c	A vulnerability has been reported due to a format string error, which could let a malicious user execute arbitrary code. Upgrades available at: http://freshmeat.net/redir/ibsh/ 57192/url_tgz/ibsh-0.3d.tar.gz Currently, we are not aware of any exploits for this vulnerability.	Iron Bars SHell Format String CAN-2005-1738	High	Security Focus, 13720, May 24, 2005

Julian Field MailScanner 4.41.3 & prior	A vulnerability has been reported due to improper reporting of viruses in certain types of zip files, which could let a remote malicious user bypass the anti-virus filter. Update available at: http://www.sng.ecs.soton.ac.uk/ mailscanner/downloads.shtml Currently we are not aware of any exploits for this vulnerability.	MailScanner Zip Files Virus Report Failure CAN-2005-1706	Medium	Security Tracker Alert ID: 1014024, May 21, 2005
KDE KDE 3.2-3.2.3, 3.3-3.3.2, 3.4, KDE Quanta 3.1	A vulnerability has been reported due to a design error in Kommander, which could let a remote malicious user execute arbitrary code. Patches available at: ftp://ftp.kde.org/pub/kde/ security_patches/f **Gentoo: http://security.gentoo.org/ glsa/glsa-200504-23.xml** Fedora: http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/3/ Ubuntu: http://security.ubuntu.com/ Subunit/pool/universe /k/kdewebdev/ Conectiva: ftp://atualizacoes.conectiva.com.br/ Currently we are not aware of any exploits for this vulnerability.	KDE Kommander Remote Arbitrary Code Execution CAN-2005-0754	High	KDE Security Advisory, April 20, 2005 Gentoo Linux Security Advisory, GLSA 200504-23, April 22, 200 Fedora Update Notification FEDORA-2005-345, April 28, 2005 Ubuntu Security Notice, USN-115-1, May 03, 2005 Conectiva Linux Security Announcement, CLA-2005:953, May 17, 2005 **Gentoo Linux Security Advisory [UPDATE] GLSA 200504-23:02, May 20, 2005**
LibTIFF LibTIFF 3.4, 3.5.1-3.5.5, 3.5.7, 3.6 .0, 3.6.1, 3.7, 3.7.1	A buffer overflow vulnerability has been reported in the 'TIFFOpen()' function when opening malformed TIFF files, which could let a remote malicious user execute arbitrary code. Patches available at: http://bugzilla.remotesensing.org/ attachment.cgi?id=238 Gentoo: http://security.gentoo.org/ glsa/glsa-200505-07.xml Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/t/tiff/ Currently we are not aware of any exploits for this vulnerability.	LibTIFF TIFFOpen Remote Buffer Overflow CAN-2005-1472	High	Gentoo Linux Security Advisory, GLSA 200505-07, May 10, 2005 Ubuntu Security Notice, USN-130-1, May 19, 2005

Linux kernel 2.6.11 .7	A Denial of Service vulnerability has been reported due to the creation of an insecure file by the kernel it87 and via686a drivers. Patch available at: http://kernel.org/pub/linux/kernel/v2.6/patch-2.6.11.8.bz2 **Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/** There is no exploit code required.	Linux Kernel it87 & via686a Drivers Denial of Service CAN-2005-1369	Low	Secunia Advisory, SA15204, May 2, 2005 **Ubuntu Security Notice, USN-131-1, May 23, 2005**
Marc Lehmann Convert-UUlib 1.50	A buffer overflow vulnerability has been reported in the Convert::UUlib module for Perl due to a boundary error, which could let a remote malicious user execute arbitrary code. Update available at: http://search.cpan.org/dist/Convert-UUlib/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-26.xml **Debian: http://security.debian.org/pool/updates/main/libc/libconvert-uulib-perl/** Currently we are not aware of any exploits for this vulnerability.	Convert-UUlib Perl Module Buffer Overflow CAN-2005-1349	High	Gentoo Linux Security Advisory, GLSA 200504-26, April 26, 2005 Secunia Advisory, SA15130, April 27, 2005 **Debian Security Advisory, DSA 727-1, May 20, 2005**
Mozilla.org Firefox 1.0	A vulnerability exists when a predictable name is issued for the plugin temporary directory, which could let a malicious user cause a Denial of Service or modify system/user information. Update available at: http://www.mozilla.org/products/firefox/all.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-10.xml SuSE: ftp://ftp.suse.com/pub/suse/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo:	Mozilla Firefox Predictable Plugin Temporary Directory CAN-2005-0578	Medium	Mozilla Foundation Security Advisory, 2005-28, February 25, 2005 SUSE Security Announcement, SUSE-SA:2005:016, March 16, 2005 Fedora Update Notification, FEDORA-2005-247 2005-03-23 Gentoo Linux Security Advisory, GLSA 200503-30 & GLSA 200503-032, March 25, 2005 **Fedora Legacy Update Advisory, FLSA:152883, May 18, 2005**

	http://security.gentoo.org/glsa/glsa-200503-30.xml http://security.gentoo.org/glsa/glsa-200503-32.xml **FedoraLegacy:** **http://download.fedoralegacy.org/\redhat/** An exploit has been published.			
Multiple Vendors ImageMagick 6.0-6.0.8, 6.1-6.1.8, 6.2 .0.7, 6.2 .0.4, 6.2, 6.2.1	A buffer overflow vulnerability has been reported due to a failure to properly validate user-supplied string lengths before copying into static process buffers, which could let a remote malicious user cause a Denial of Service. Upgrades available at: http://www.imagemagick.org/script/binary-releases.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/i/imagemagick/** A Proof of Concept exploit has been published.	ImageMagick Remote Buffer Overflow CAN-2005-1275	Low	Security Focus, 13351, April 25, 2005 Fedora Update Notification FEDORA-2005-344, April 28, 2005 **Ubuntu Security Notice, USN-132-1 May 23, 2005, May 23, 2005**
Multiple Vendors KDE 2.0, beta, 2.0.1, 2.1-2.1.2, 2.2-2.2.2, 3.0-3.0.5, 3.1-3.1.5, 3.2-3.2.3, 3.3-3.3.2, 3.4; Novell Linux Desktop 9; SuSE Linux 9.1, x86_64, 9.2, x86_64, 9.3, Linux Enterprise Server 9	A buffer overflow vulnerability has been reported in the 'kimgio' image library due to insufficient validation of PCX image data, which could let a remote malicious user cause a Denial of Service or possibly execute arbitrary code. Patches available at: http://bugs.kde.org/attachment.cgi?id=10325&action=view http://bugs.kde.org/attachment.cgi?id=10326&action=view **SuSE:** **ftp://ftp.suse.com/pub/suse/** Gentoo: http://security.gentoo.org/glsa/glsa-200504-22.xml Debian: http://security.debian.org/pool/updates/main/k/kdelibs/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/	KDE 'kimgio' image library Remote Buffer Overflow CAN-2005-1046	High	SUSE Security Announcement, SUSE-SA:2005:022, April 11, 2005 Gentoo Linux Security Advisory, GLSA 200504-22, April 22, 2005 Debian Security Advisory, DSA 714-1, April 26, 2005 Fedora Update Notification, FEDORA-2005-350, May 2, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:085, May 12, 2005 Conectiva Linux Security Announcement, CLA-2005:953, May 17,

	Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/k/kdelibs/ Mandriva: http://www.mandriva.com/security/advisories Conectiva: ftp://atualizacoes.conectiva.com.br/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-393.html Denial of Service Proofs of Concept exploits have been published.			2005 RedHat Security Advisory, RHSA-2005:393-05, May 17, 2005 **SUSE Security Summary Report, SUSE-SR:2005:013, May 18, 2005**
Multiple Vendors MandrakeSoft Corporate Server 3.0, x86_64, Linux Mandrake 10.0, AMD64, 10.1, X86_64;Novell Evolution 2.0.2l Ubuntu Linux 4.1 ppc, ia64, ia32; Ximian Evolution 1.0.3-1.0.8, 1.1.1, 1.2-1.2.4, 1.3.2 (beta)	A buffer overflow vulnerability exists in the main() function of the 'camel-lock-helper.c' source file, which could let a remote malicious user execute arbitrary code. Update available at: http://cvs.gnome.org/viewcvs/evolution/camel/camel-lock-helper.c?rev=1.7&hideattic=0&view=log Gentoo: http://security.gentoo.org/glsa/glsa-200501-35.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/e/evolution/ SUSE: ftp://ftp.suse.com/pub/suse/ Debian: http://security.debian.org/pool/updates/main/e/evolution/ Conectiva: ftp://atualizacoes.conectiva.com.br/ ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-238.html** Currently we are not aware of any exploits for this vulnerability.	Evolution Camel-Lock-Helper Application Remote Buffer Overflow CAN-2005-0102	High	Gentoo Linux Security Advisory, GLSA 200501-35, January 25, 2005 Ubuntu Security Notice, USN-69-1, January 25, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:024, January 27, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 Debian Security Advisory, DSA 673-1, February 10, 2005 Conectiva Linux Security Announcement, CLA-2005:925, February 16, 2005 ALTLinux Security Advisory, March 29, 2005 **RedHat Security Advisory, RHSA-2005:238-18, May 19, 2005**

Multiple Vendors Qpopper 4.x; Gentoo Linux	Several vulnerabilities have been reported: a vulnerability was reported because user supplied config and trace files are processed with elevated privileges, which could let a malicious user create/overwrite arbitrary files; and a vulnerability was reported due to an unspecified error which could let a malicious user create group or world-writable files. Upgrades available at: ftp://ftp.qualcomm.com/eudora/servers/unix/popper/old/qpopper4.0.5.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200505-17.xml There is no exploit code required.	Qpopper Multiple Insecure File Handling CAN-2005-1151 CAN-2005-1152	Medium	Gentoo Linux Security Advisory GLSA 200505-17, May 23, 2005 Secunia Advisory, SA15475, May 24, 2005
Multiple Vendors Gentoo Linux; GNU GDB 6.3	Multiple vulnerabilities have been reported: a heap overflow vulnerability was reported when loading malformed object files, which could let a remote malicious user execute arbitrary code; and a vulnerability was reported which could let a malicious user obtain elevated privileges. Gentoo: http://security.gentoo.org/glsa/glsa-200505-15.xml Currently we are not aware of any exploits for these vulnerabilities.	GDB Multiple Vulnerabilities CAN-2005-1704 CAN-2005-1705	High	Gentoo Linux Security Advisory, GLSA 200505-15, May 20, 2005
Multiple Vendors GraphicsMagick GraphicsMagick 1.0, 1.0.6, 1.1, 1.1.3-1.1.6; ImageMagick ImageMagick 5.3.3, 5.3.8, 5.4.3, 5.4.4 .5, 5.4.7, 5.4.8, 5.5.3.2-1.2.0, 5.5.4, 5.5.6 .0-20030409, 5.5.6, 5.5.7, 6.0-6.0.8, 6.1-6.1.8, 6.2.0.7, 6.2 .0.4, 6.2-6.2.2	A remote Denial of Service vulnerability has been reported due to a failure to handle malformed XWD image files. Gentoo: http://security.gentoo.org/glsa/glsa-200505-16.xml Currently we are not aware of any exploits for this vulnerability.	ImageMagick & GraphicsMagick XWD Decoder Remote Denial of Service CAN-2005-1739	Low	Gentoo Linux Security Advisory, GLSA 200505-16, May 21, 2005
Multiple Vendors Linux kernel 2.2.x, 2.4.x, 2.6.x	A buffer overflow vulnerability has been reported in the 'elf_core_dump()' function due to a signedness error, which could let a malicious user execute arbitrary code with ROOT privileges. Update available at: http://kernel.org/ Trustix: http://www.trustix.org/	Linux Kernel ELF Core Dump Buffer Overflow CAN-2005-1263	High	Secunia Advisory, SA15341, May 12, 2005 Trustix Secure Linux Security Advisory, 2005-0022, May 13, 2005 **Ubuntu Security Notice, USN-131-1,**

	errata/2005/0022/ **Ubuntu:** **http://security.ubuntu.com/ ubuntu/pool/main/l/** An exploit script has been published.			**May 23, 2005**
Multiple Vendors Linux Kernel 2.6 up to & including 2.6.12-rc4	Several vulnerabilities have been reported: a vulnerability was reported in raw character devices (raw.c) because the wrong function is called before passing an ioctl to the block device, which crosses security boundaries by making kernel address space accessible from user space; and a vulnerability was reported in the 'pkt_ioctl' function in the 'pktcdvd' block device ioctl handler (pktcdvd.c) because the wrong function is called before passing an ioctl to the block device, which could let a malicious user execute arbitrary code. Update available at: http://kernel.org/ **Ubuntu:** **http://security.ubuntu.com/ ubuntu/pool/main/l/** A Proof of Concept Denial of Service exploit script has been published.	Multiple Vendor Linux Kernel pktcdvd & raw device Block Device CAN-2005-1264 CAN-2005-1589	High	Secunia Advisory, SA15392, May 17, 2005 **Ubuntu Security Notice, USN-131-1, May 23, 2005**
Multiple Vendors Linux kernel 2.6.10, 2.6, -test1-test11, 2.6.1-2.6.12; RedHat Desktop 3.0, Enterprise Linux WS 3, ES 3, AS 3	A Denial of Service vulnerability has been reported on 64-bit platform due to a flaw in offset handling for the extended attribute file system code. RedHat: http://rhn.redhat.com/ errata/RHSA-2005-294.html Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 64 Bit EXT3 Filesystem Extended Attribute Denial of Service CAN-2005-0757	Low	RedHat Security Advisory, RHSA-2005:294-29, May 18, 2005
Multiple Vendors Linux kernel 2.6.10, 2.6, -test9-CVS, -test1-test11, 2.6.1-2.6.9; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	A Denial of Service vulnerability has been reported in the 'fib_seq_start' function in 'fib_hash.c.' RedHat; http://rhn.redhat.com/ errata/RHSA-2005-366.html **Ubuntu:** **http://security.ubuntu.com/ ubuntu/pool/main/l/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 'Fib_Seq_Start' Denial of Service CAN-2005-1041	Low	RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 **Ubuntu Security Notice, USN-131-1, May 23, 2005**

Multiple Vendors Linux kernel 2.6.10, 2.6.11.5-2.6.11 .8, 2.6.11, -rc2-rc4	A Denial of Service vulnerability has been reported due to a race condition in the 'key_user_lookup()' function (only on SMP capable systems). Ubuntu: http://security.ubuntu.com/ ubuntu/pool/main/l/ Currently we are not aware of any exploits for this vulnerability.	Linux Kernel 'Key_User_Lookup()' Denial of Service CAN-2005-1368	Low	Ubuntu Security Notice, USN-131-1, May 23, 2005
Multiple Vendors Squid Web Proxy Cache 2.0 PATCH2, 2.1 PATCH2, 2.3 STABLE5, 2.3 STABLE4, 2.4 STABLE7, 2.4 STABLE6, 2.4, STABLE2, 2.5 STABLE3-STABLE7, 2.5 STABLE1	A vulnerability has been reported due to a failure to handle CR/LF characters in HTTP requests, which could let a remote malicious user poison the web proxy cache. Patches available at: http://www.squid-cache.org/ Versions/v2/2.5/squid-2.5.STABLE9.tar.gz **Fedora:** **http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/3/** There is no exploit code required.	Squid Proxy HTTP Response Splitting Remote Cache Poisoning CAN-2005-0175	Medium	Squid Proxy Cache Security Update Advisory, SQUID-2005:5, April 23, 2005 **Fedora Update Notification, FEDORA-2005-373, May 17, 2005**
Multiple Vendors Squid Web Proxy Cache 2.0 PATCH2, 2.1 PATCH2, 2.3 STABLE5, 2.3 STABLE4, 2.4 STABLE7, 2.4 STABLE6, 2.4, STABLE2, 2.5 STABLE3-STABLE7, 2.5 STABLE1	A vulnerability has been reported when handling upstream HTTP agents, which could let a remote malicious user poison the web proxy cache. Patches available at: http://www.squid-cache.org/ Versions/v2/2.5/squid-2.5.STABLE9.tar.gz **Fedora:** **http://download.fedora.redhat.com/ pub/fedora/linux/core/updates/3/** There is no exploit code required.	Squid Proxy Remote Cache Poisoning CAN-2005-0174	Medium	Squid Proxy Cache Security Update Advisory, SQUID-2005:4, April 23, 2005 **Fedora Update Notification, FEDORA-2005-373, May 17, 2005**
Net-snmp Net-snmp 5.x	A vulnerability has been reported in 'fixproc' due to a failure to securely create temporary files in world writable locations, which could let a malicious user obtain elevated privileges and possibly execute arbitrary code. Gentoo: http://security.gentoo.org/ glsa/glsa-200505-18.xml There is no exploit code required.	Net-SNMP Fixprox Insecure Temporary File Creation CAN-2005-1740	High	Gentoo Linux Security Advisory, GLSA 200505-18, May 23, 2005

Petr Vandrovec ncpfs prior to 2.2.6	Two vulnerabilities exist: a vulnerability exists in 'ncpfs-2.2.0.18/lib/ncplib.c' due to improper access control in the 'ncp_fopen_nwc()' function, which could let a malicious user obtain unauthorized access; and a buffer overflow vulnerability exists in 'ncpfs-2.2.5/sutil/ncplogin.c' due to insufficient validation of the 'opt_set_volume_after_parsing_all_options()' function, which could let a malicious user execute arbitrary code. Update available at: ftp://platan.vc.cvut.cz/pub/linux/ncpfs/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-44.xml Debian: http://www.debian.org/security/2005/dsa-665 Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.SUSE.com/pub/SUSE **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-371.html** An exploit script has been published.	Petr Vandrovec ncpfs Access Control & Buffer Overflow CAN-2005-0013 CAN-2005-0014	High	Security Tracker Alert ID: 1013019, January 28, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:028, February 2, 2005 Debian Security Advisory, DSA-665-1, February 4, 2005 SUSE Security Summary Report, SUSE-SR:2005:003, February 4, 2005 **RedHat Security Advisory, RHSA-2005:371-06, May 17, 2005**
Picasm Picasm 1.10, 1.12 b	A buffer overflow vulnerability has been reported due to a boundary error in the error handling, which could let a remote malicious user execute arbitrary code. Upgrade available at: http://www.co.jyu.fi/~trossi/pic/picasm112c.tar.gz An exploit script has been published.	Picasm Error Handling Buffer Overflow CAN-2005-1679	High	Securiteam, May 22, 2005
ppxp ppxp 0.2 001080415	A vulnerability has been reported because a shell can be opened with superuser privileges, which could let a malicious user obtain elevated privileges. Debian: http://security.debian.org/pool/updates/main/p/ppxp There is no exploit code required.	PPXP Local Privilege Escalation CAN-2005-0392	High	Debian Security Advisory, DSA 725-1 , May 19, 2005
Sun Microsystems, Inc. Solaris 7.0, _x86, 8.0, _x86, 9.0, _x86;	A Denial of Service vulnerability has been reported in the automountd daemon. Patches available at: http://sunsolve.sun.com/search/	Sun Solaris automountd Denial of Service	Low	Sun(sm) Alert Notification, 57786, May 10, 2005 **ASA-2005-116, May**

Avaya Interactive Response, 1.2.1, 1.3	document.do?assetkey=1-26-57786-1 **Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-116_SUN-5-13-2005.pdf** Currently we are not aware of any exploits for this vulnerability.	CAN-2005-1518		**18, 2005**
xine gxine 0.4.0-0.4.4	A format string vulnerability has been reported due to insecure implementation of a formatted printing function, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	GXINE Remote Hostname Format String CAN-2005-1692	High	pst.advisory, May 21, 2005

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Andrea Bugada PHP Advanced Transfer Manager 1.21	A vulnerability has been reported in the 'include/common.php' script if 'allow_url_fopen' is set to 'on' in the 'php.ini' configuration file, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept has been published.	PHP Advanced Transfer Manager Arbitrary Command Execution CAN-2005-1681	High	Security Tracker Alert ID: 1014008, May 19, 2005
BEA Systems WebLogic Express 6.x, 7.x, 8.x, WebLogic Portal 8.x, WebLogic Server 6.x, 7.x, 8.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to an error that can be exploited by a remote malicious user granted the Monitor security role to shrink or reset JDBC connection pools; a vulnerability was reported due to an error when handing security provider exceptions, which could let a remote malicious user manipulate the identity of threads and cause failure in the auditing of security exceptions; a vulnerability was reported because users do not need to re-authenticate after new security constraints have been deployed in web applications; a vulnerability was reported in the 'UserLogin' control after a failed login because passwords are echoed back in standard output, which could let a remote	BEA WebLogic Server & WebLogic Express Multiple Remote CAN-2005-1742 CAN-2005-1743 CAN-2005-1744 CAN-2005-1745 CAN-2005-1746 CAN-2005-1747 CAN-2005-1748 CAN-2005-1749	High	Secunia Advisory, SA15486, May 24, 2005 Security Advisories, BEA05-75.00-BEA05-082, May 24, 2005

	malicious user obtain sensitive information; a vulnerability was reported in sites running in clusters due to an error in the cookie parsing; a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of certain unspecified input, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported because it is possible to make anonymous binds to the embedded LDAP server, which could let a remote malicious user cause a Denial of Service; and a buffer overflow vulnerability was reported due to an unspecified boundary error, which could let a remote malicious user cause a Denial of Service. Updates available at: http://dev2dev.bea.com/pub/advisory/ There is no exploit code required.			
D-Link DSL-502T, DSL-504T, DSL-562T, DSL-G604T	A vulnerability has been reported due to insufficient authentication, which could let a remote malicious user obtain administrative access. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	D-Link DSL Router Remote Administrative Access CAN-2005-1680	High	Security Focus, 13679, May 19, 2005
Emilio Jose Jimenez TOPo 2.2	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'index.php' due to insufficient sanitization of the 'ID' parameter, which could let a remote malicious user execute arbitrary HTML and script code; a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of input passed to the web and e-mail fields when a comment is added, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported because data files are stored improperly in the 'data/' directory, which could let a remote malicious user obtain sensitive information No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	TOPo Multiple Input Validation CAN-2005-1715 CAN-2005-1716	High	Secunia Advisory: SA15325, May 20, 2005
Extreme Networks BlackDiamond 10808, 8800, ExtremeWare	A vulnerability has been reported due to an unspecified error which could let a remote malicious user obtain superuser shell access to the underlying XOS operating	ExtremeWare XOS Superuser Access	High	Extreme Networks Field Notice, FN0215, May 19, 2005

XOS 11.1, 11.0, 10.0	system. Upgrade information available at: http://www.extremenetworks.com/ services/documentation/FieldNotices_ FN0215-Security_Alert_EXOS.asp Currently we are not aware of any exploits for this vulnerability.	CAN-2005-1670		US-CERT VU#937838
Fusionphp Fusion SBX 1.2 & prior	A vulnerability has been reported in 'index.php' because the 'extract()' function is used insecurely, which could let a remote malicious user bypass authentication and execute arbitrary code. No workaround or patch available at time of publishing. **An exploit script has been published.**	Fusion SBX Authentication Bypass & Arbitrary Code Execution **CAN-2005-1596**	High	Secunia Advisory, SA15257, May 10, 2005 **Security Focus, 13661, May 17, 2005**
Gearbox Software Halo Combat Evolved 1.6	A remote Denial of Service vulnerability has been reported when processing malformed data. No workaround or patch available at time of publishing. An exploit script has been published.	Gearbox Software Halo Game Server Remote Denial of Service CAN-2005-1741	Low	Security Focus, 13728, May 24, 2005
Help Center Live Help Center Live 1.0, 1.2-1.2.7	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in 'index.php' due to insufficient sanitization of the 'find' parameter, which could let a remote malicious user execute arbitrary HTML and script code; a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of input passed to the name and message fields when requesting a chat and in the message body when opening a trouble ticket, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported due to insufficient sanitization of certain input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability was reported because it is possible to trick an administrator into performing certain actions when a specially crafted URL is accessed. The vulnerabilities have reportedly been fixed by the vendor. There is no exploit code required; however, Proofs of Concept exploits have been published.	Help Center Live Multiple Input Validation CAN-2005-1672 CAN-2005-1673 CAN-2005-1674	High	GulfTech Security Research Advisory, May 17, 2005

Metro Marketing Cookie Cart 4.x	Several vulnerabilities have been reported: a vulnerability was reported in the 'testmy.cgi' and 'testmy.pl' scripts which could let a remote malicious user obtain sensitive information; and a vulnerability was reported because a remote malicious user can obtain the password that contains encrypted passwords. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	Cookie Cart Information Disclosure CAN-2005-1732 CAN-2005-1733	Medium	Security Tracker Alert, 1014026, May 22, 2005
Mozilla.org Mozilla Browser 1.0-1.0.2, 1.1-1.7.6, Firefox 0.8-0.10.1, 1.0.1, 1.0.2; Netscape Navigator 7.0, 7.0.2, 7.1, 7.2, 7.0-7.2	Multiple vulnerabilities have been reported: a vulnerability was reported in the 'EMBED' tag for non-installed plugins when processing the 'PLUGINSPAGE' attribute due to an input validation error, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because blocked popups that are opened through the GUI incorrectly run with 'chrome' privileges, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because the global scope of a window or tab are not cleaned properly before navigating to a new web site, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because the URL of a 'favicons' icon for a web site isn't verified before changed via JavaScript, which could let a remote malicious user execute arbitrary code with elevated privileges; a vulnerability was reported because the search plugin action URL is not properly verified before used to perform a search, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to the way links are opened in a sidebar when using the '_search' target, which could let a remote malicious user execute arbitrary code; several input validation vulnerabilities were reported when handling invalid type parameters passed to 'InstallTrigger' and 'XPInstall' related objects, which could let a remote malicious user execute arbitrary code; and vulnerabilities were reported due to insufficient validation of DOM nodes in certain privileged UI code, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.mozilla.org/products/firefox/ http://www.mozilla.org/	Mozilla Suite / Firefox Multiple Vulnerabilities CAN-2005-0752 CAN-2005-1153 CAN-2005-1154 CAN-2005-1155 CAN-2005-1156 CAN-2005-1157 CAN-2005-1158 CAN-2005-1159 CAN-2005-1160	High	Mozilla Foundation Security Advisories, 2005-35 - 2005-41, April 16, 2005 Gentoo Linux Security Advisory, GLSA 200504-18, April 19, 2005 US-CERT VU#973309 RedHat Security Advisories, RHSA-2005:383-07 & RHSA-2005-386., April 21 & 26, 2005 Turbolinux Security Advisory, TLSA-2005-49, April 21, 2005 US-CERT VU#519317 SUSE Security Announcement, SUSE-SA:2005:028, April 27, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 Ubuntu Security Notice, USN-124-1 & USN-124-2, May 11 & 12, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:088, May 14, 2005

	products/mozilla1.x/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-18.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-383.html http://rhn.redhat.com/errata/RHSA-2005-386.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/m/mozilla-firefox/ **Mandriva: http://www.mandriva.com/security/advisories** **FedoraLegacy: http://download.fedoralegacy.org/redhat/** **An exploit script has been published.**			**Mandriva Linux Security Update Advisory, MDKSA-2005:088-1, May 17, 2005** **Fedora Legacy Update Advisory, FLSA:152883, May 18, 2005** **PacketStorm, May 23, 2005**
Mozilla.org Mozilla Browser Suite prior to 1.7.6 ; Thunderbird prior to 1.0.2 ; Firefox prior to 1.0.2	A buffer overflow vulnerability has been reported due to a boundary error in the GIF image processing of Netscape extension 2 blocks, which could let a remote malicious user execute arbitrary code. Mozilla Browser Suite; http://www.mozilla.org/products/mozilla1.x/ Thunderbird: http://download.mozilla.org/?product=thunderbird-1.0.2&os=win⟨=en-US Firefox: http://www.mozilla.org/products/firefox/	Mozilla Suite/ Firefox/ Thunderbird GIF Image Processing Remote Buffer Overflow CAN-2005-0399	High	Mozilla Foundation Security Advisory 2005-30, March 23, 2005 US-CERT VU#557948 **Fedora Legacy Update Advisory, FLSA:152883, May 18, 2005**

	Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.000123 **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for this vulnerability.			
Mozilla.org Mozilla Suite prior to 1.7.6, Firefox prior to 1.0.2	A vulnerability has been reported when processing drag and drop operations due to insecure XUL script loading, which could let a remote malicious user execute arbitrary code. Mozilla Browser: http://www.mozilla.org/products/mozilla1.x/ Firefox: http://www.mozilla.org/products/firefox/ Fedora: http://download.fedora.red hat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml http://security.gentoo.org/glsa/glsa-200503-31.xml Slackware: http://slackware.com/security/viewer.php?El=slackware-security&ay=2005&m=slackware-security.000123 RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ **Mandriva:**	Mozilla Suite/ Firefox Drag and Drop Arbitrary Code Execution CAN-2005-0401	High	Mozilla Foundation Security Advisory 2005-32, March 23, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:088, May 14, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:088-1, May 17, 2005** **Fedora Legacy Update Advisory, FLSA:152883, May 18, 2005**

	http://www.mandriva.com/security/advisories **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** A Proof of Concept exploit has been published.			
Mozilla Firefox 1.0	A vulnerability exists in the XPCOM implementation that could let a remote malicious user execute arbitrary code. The exploit can be automated in conjunction with other reported vulnerabilities so no user interaction is required. A fixed version (1.0.1) is available at: http://www.mozilla.org/products/firefox/all.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml SGI: ftp://patches.sgi.com/support/free/security/advisories/ **Mandriva:** **http://www.mandriva.com/security/advisories** **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** A Proof of Concept exploit has been published.	Mozilla Firefox Remote Code Execution Vulnerability CAN-2005-0527	High	Security Tracker Alert ID: 1013301, February 25, 2005 Gentoo Linux Security Advisory GLSA 200503-30. March 25, 2005 SGI Security Advisory, 20050501 -01-U, May 5, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:088, May 14, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:088-1, May 17, 2005** **Fedora Legacy Update Advisory, FLSA:152883, May 18, 2005**
Mozilla Firefox Preview Release, 0.8, 0.9 rc, 0.9-0.9.3, 0.10, 0.10.1, 1.0-1.0.3	Several vulnerabilities have been reported: a vulnerability was reported due to insufficient protection of 'IFRAME' JavaScript URLS from being executed in the context of another history list URL, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability was reported in 'InstallTrigger .install()' due to insufficient verification of the 'Icon URL' parameter, which could let a remote malicious user execute arbitrary JavaScript code. Workaround: Disable "tools/options/web-Features/>Allow web sites to install software"	Mozilla Firefox Remote Arbitrary Code Execution CAN-2005-1476 CAN-2005-1477	High	Secunia Advisory, SA15292, May 9, 2005 US-CERT VU#534710 US-CERT VU#648758 Slackware Security Advisory, SSA:2005-135-01, May 15, 2005 Gentoo Linux Security Advisory, GLSA 200505-11, May 16, 2005

	Slackware: ftp://ftp.slackware.com/pub/slac ware/ Gentoo: http://security.gentoo.org/glsa/glsa-200505-11.xml TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-434.html** **http://rhn.redhat.com/errata/RHSA-2005-435.html** Proofs of Concept exploit scripts have been published.			Turbolinux Security Advisory, TLSA-2005-56, May 16, 2005 **RedHat Security Advisories, RHSA-2005:434-10 & RHSA-2005:435-10, May 23 & 24, 2005**
Mozilla Mozilla 0.x, 1.0, 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7.x Mozilla Firefox 0.x Mozilla Thunderbird 0.x	Multiple vulnerabilities exist in Firefox, Mozilla and Thunderbird that can permit users to bypass certain security restrictions, conduct spoofing and script insertion attacks and disclose sensitive and system information. Mozilla: Update to version 1.7.5: http://www.mozilla.org/products/mozilla1.x/ Firefox: Update to version 1.0: http://www.mozilla.org/products/firefox/ Thunderbird: Update to version 1.0: http://www.mozilla.org/products/thunderbird/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?El=slackware-security&y=2005&m=slackware-security.000123 RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html SGI: ftp://patches.sgi.com/support/free/security/advisories/	Mozilla Firefox, Mozilla, and Thunderbird Multiple Vulnerabilities CAN-2005-0141 CAN-2005-0143 CAN-2005-0144 CAN-2005-0145 CAN-2005-0146 CAN-2005-0147 CAN-2005-0148 CAN-2005-0149 CAN-2005-0150	High	Mozilla Foundation Security Advisory 2005-01, 03, 04, 07, 08, 09, 10, 11, 12 Fedora Update Notification, FEDORA-2005-248, 249, 251, 253, March 23 & 25, 2005 Slackware Security Advisory, SSA:2005-085-01, March 27, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:088, May 14, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:088-1, May 17, 2005**

	Mandriva: **http://www.mandriva.com/security/advisories** **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for these vulnerabilities.		**Fedora Legacy Update Advisory, FLSA:152883, May 18, 2005**

Mozilla Mozilla 1.7.x and prior Mozilla Firefox 1.x and prior Mozilla Thunderbird 1.x and prior Netscape Netscape 7.2	Multiple vulnerabilities exist in Firefox, Mozilla and Thunderbird. These can be exploited by malicious, local users to perform certain actions on a vulnerable system with escalated privileges and by malicious people to conduct spoofing attacks, disclose and manipulate sensitive information, and potentially compromise a user's system. Firefox: Update to version 1.0.1: http://www.mozilla.org/products/firefox/ Mozilla: The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.7.6 version. Thunderbird: The vulnerabilities have been fixed in the CVS repository and will be included in the upcoming 1.0.1 version. Fedora update for Firefox: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Red Hat: http://rhn.redhat.com/errata/RHSA-2005-176.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml http://security.gentoo.org/glsa/glsa-200503-32.xml Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.000123 SGI: ftp://patches.sgi.com/support/free/security/advisories/	Mozilla / Firefox / Thunderbird Multiple Vulnerabilities CAN-2005-0255 CAN-2005-0584 CAN-2005-0585 CAN-2005-0587 CAN-2005-0588 CAN-2005-0589 CAN-2005-0590 CAN-2005-0592 CAN-2005-0593	High	Mozilla Foundation Security Advisories 2005-14, 15, 17, 18, 19, 20, 21, 24, 28 Red Hat RHSA-2005:176-11, March 1, 2005 Gentoo, GLSA 200503-10, March 4, 2005 SUSE Security Announcement, SUSE-SA:2005:016, March 16, 2005 Fedora Update Notification, FEDORA-2005-248, 249, 251, & 253, March 23 & 25, 2005 Gentoo Linux Security Advisory, GLSA 200503-30 & GLSA 200503-032, March 25, 2005 Slackware Security Advisory, SSA:2005-085-01, March 27, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 **Fedora Legacy Update Advisory, FLSA:152883, May 18, 2005**

	FedoraLegacy: **http://download.fedoralegacy.org/redhat/** Currently we are not aware of any exploits for these vulnerabilities.			
Mozilla Mozilla Browser prior to 1.7.8; Mozilla Suite prior to 1.7.8; Firefox prior to 1.0.4; Firebird 0.5, 0.6.1, 0.7	A vulnerability was reported due to a failure in the application to properly verify Document Object Model (DOM) property values, which could let a remote malicious user execute arbitrary code. Firefox: http://www.mozilla.org/products/firefox/ Mozilla Browser Suite: http://www.mozilla.org/products/mozilla1.x/ TurboLinux:: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-434.html** **http://rhn.redhat.com/errata/RHSA-2005-435.html** Currently we are not aware of any exploits for this vulnerability.	Mozilla Suite And Firefox DOM Property Overrides CAN-2005-1532	High	Mozilla Foundation Security Advisory, 2005-44, May 12, 2005 Turbolinux Security Advisory, TLSA-2005 -56, May 16, 2005 **RedHat Security Advisories, RHSA-2005:434-10 & RHSA-2005:435-10, May 23 & 24, 2005**
Mozilla Mozilla Browser prior to 1.7.8; Mozilla Suite prior to 1.7.8; Firefox prior to 1.0.4; Firebird 0.5, 0.6.1, 0.7	A vulnerability was reported when processing 'javascript:' URLs, which could let a remote malicious user execute arbitrary code. Firefox: http://www.mozilla.org/products/firefox/ Mozilla Browser Suite: http://www.mozilla.org/products/mozilla1.x/ TurboLinux:: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-434.html** **http://rhn.redhat.com/errata/RHSA-2005-435.html** Currently we are not aware of any exploits for this vulnerability.	Mozilla Suite And Firefox Wrapped 'javascript:' URLs CAN-2005-1531	High	Mozilla Foundation Security Advisory, 2005-43, May 12, 2005 Turbolinux Security Advisory, TLSA-2005-56, May 16, 2005 **RedHat Security Advisories, RHSA-2005:434-10 & RHSA-2005:435-10, May 23 & 24, 2005**

Mozilla Mozilla Firefox 1.0 and 1.0.1	A vulnerability exists that could let remote malicious users conduct Cross-Site Scripting attacks. This is due to missing URI handler validation when dragging an image with a "javascript:" URL to the address bar. Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ **Mandriva:** **http://www.mandriva.com/security/advisories** **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** A Proof of Concept exploit has been published.	Mozilla Firefox Image Javascript URI Dragging Cross-Site Scripting Vulnerability CAN-2005-0591	High	Secunia SA14406, March 1, 2005 Gentoo Linux Security Advisory, GLSA 200503-30, March 25, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 **Mandriva Linux Security Update, MDKSA-2005:088-1, Advisory, May 17, 2005** **Fedora Legacy Update Advisory, FLSA:152883, May 18, 2005**
Multiple Vendors DeleGate DeleGate 7.7 .0, 7.7.1, 7.8 .0-7.8.2, 7.9.11, 8.3.3, 8.3.4, 8.4 .0, 8.5 .0, 8.9-8.9.6, 8.10-8.10.2; dnrd dnrd 1.0-1.4, 2.0-2.10; PowerDNS PowerDNS 2.0 RC1, 2.8, 2.9.15, 2.9.16	A remote Denial of Service vulnerability has been reported when handling a specially crafted DNS message. Contact your vendor for updates. Currently we are not aware of any exploits for this vulnerability.	Multiple Vendor DNS Message Decompression Remote Denial of Service CAN-2005-0036 CAN-2005-0037 CAN-2005-0038	Low	NISCC Vulnerability Advisory, DNS - 589088, May 24, 2005

Multiple Vendors
Mozilla Firefox 1.0;
Gentoo Linux;
Thunderbird 0.6, 0.7-0.7.3, 0.8, 0.9, 1.0, 1.0.1;
Netscape Netscape 7.2
	There are multiple vulnerabilities in Mozilla Firefox. A remote user may be able to cause a target user to execute arbitrary operating system commands in certain situations or access access content from other windows, including the 'about:config' settings. This is due to a hybrid image vulnerability that allows batch statements to be dragged to the desktop and because tabbed javascript vulnerabilities let remote users access other windows.
	A fix is available via the CVS repository
	Fedora:
	ftp://aix.software.ibm.com/aix/efixes/security/perl58x.tar.Z
	Red Hat:
	http://rhn.redhat.com/errata/
		Mozilla Firefox Multiple Vulnerabilities
		CAN-2005-0230
		CAN-2005-0231
		CAN-2005-0232
			High	Security Tracker Alert ID: 1013108, February 8, 2005
				Fedora Update Notification, FEDORA-2005-182, February 26, 2005
				Red Hat RHSA-2005:176-11, March 1, 2005
				Gentoo, GLSA 200503-10, March 4, 2005
				Security Focus, 12468, March 22, 2005
				Gentoo Linux Security

	RHSA-2005-176.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml Thunderbird: http://download.mozilla.org/?product=thunderbird-1.0.2&os=win<=en-US Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html SGI: ftp://patches.sgi.com/support/free/security/advisories/ **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** A Proof of Concept exploit has been published.			Advisory, GLSA 200503-30, March 25, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 SGI Security Advisory, 20050501-01-U, May 5, 2005 **Fedora Legacy Update Advisory, FLSA:152883, May 18, 2005**
Multiple Vendors Mozilla.org Mozilla Browser 1.7.6, Firefox 1.0.1, 1.0.2; K-Meleon K-Meleon 0.9; Netscape 7.2; K-Meleon 0.9	A vulnerability has been reported in the javascript implementation due to improper parsing of lamba list regular expressions, which could a remote malicious user obtain sensitive information. The vendor has issued a fix, available via CVS. RedHat: http://rhn.redhat.com/errata/RHSA-2005-383.html http://rhn.redhat.com/errata/RHSA-2005-386.html Slackware: http://www.mozilla.org/projects/security/known-vulnerabilities.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ SUSE: ftp://ftp.SUSE.com/pub/SUSE RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html	Mozilla Suite/Firefox JavaScript Lambda Information Disclosure CAN-2005-0989	Medium	Security Tracker Alert, 1013635, April 4, 2005 Security Focus, 12988, April 16, 2005 RedHat Security Advisories, RHSA-2005:383-07 & RHSA-2005:386-08, April 21 & 26, 2005 Turbolinux Security Advisory, TLSA-2005-49, April 21, 2005 Slackware Security Advisory, SSA:2005-111-04, April 22, 2005 SUSE Security Announcement, SUSE-SA:2005:028, April 27, 2005 RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005 SGI Security Advisory, 20050501-01-U, May 5,

	SGI: ftp://patches.sgi.com/support/free/security/advisories/ **Mandriva:** **http://www.mandriva.com/security/advisories** **FedoraLegacy:** **http://download.fedoralegacy.org/redhat/** There is no exploit code required; however, a Proof of Concept exploit has been published.			2005 Mandriva Linux Security Update Advisory, MDKSA-2005:088, May 14, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:088-1, May 17, 2005** **Fedora Legacy Update Advisory, FLSA:152883, May 18, 2005**
Multiple Vendors Squid Web Proxy Cache2.5.STABLE9 & prior	A vulnerability has been reported in the DNS client when handling DNS responses, which could let a remote malicious user spoof DNS lookups. Patch available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE9-dns_query-4.patch Trustix: http://www.trustix.org/errata/2005/0022/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** **Ubuntu:** **http://security.ubuntu.com/ubuntu/pool/main/s/squid/** Currently we are not aware of any exploits for this vulnerability.	Squid Proxy DNS Spoofing CAN-2005-1519	Medium	Security Focus, 13592, May 11, 2005 Trustix Secure Linux Security Advisory, 2005-0022, May 13, 2005 **Fedora Update Notification, FEDORA-2005-373, May 17, 2005** **Ubuntu Security Notice, USN-129-1 May 18, 2005**
Multiple Vendors ALT Linux Compact 2.3, Junior 2.3; Apple Mac OS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8, Mac OS X Server 10.0, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8; MIT Kerberos 5 1.0, 5 1.0.6, 5 1.0.8, 51.1-5 1.4; Netkit Linux Netkit 0.9-0.12, 0.14-0.17, 0.17.17; Openwall GNU/*/Linux (Owl)-current, 1.0, 1.1; FreeBSD 4.10-PRERELEASE, 2.0, 4.0 .x, -RELENG,	Two buffer overflow vulnerabilities have been reported in Telnet: a buffer overflow vulnerability has been reported in the 'slc_add_reply()' function when a large number of specially crafted LINEMODE Set Local Character (SLC) commands is submitted, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability has been reported in the 'env_opt_add()' function, which could let a remote malicious user execute arbitrary code. ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Apple: http://wsidecar.apple.com/cgi-bin/	Telnet Client 'slc_add_reply()' & 'env_opt_add()' Buffer Overflows CAN-2005-0468 CAN-2005-0469	High	iDEFENSE Security Advisory, March 28, 2005 US-CERT VU#291924 Mandrakelinux Security Update Advisory, MDKSA-2005:061, March 30, 2005 Gentoo Linux Security Advisories, GLSA 200503-36 & GLSA 200504-01, March 31 & April 1, 2005 Debian Security Advisory, DSA 703-1, April 1, 2005

alpha, 4.0, 4.1, 4.1.1 -STABLE, -RELEASE, 4.1.1, 4.2, -STABLEpre122300, -STABLEpre050201, 4.2 -STABLE, -RELEASE, 4.2, 4.3 -STABLE, -RELENG, 4.3 -RELEASE-p38, 4.3 -RELEASE, 4.3, 4.4 -STABLE, -RELENG, -RELEASE-p42, 4.4, 4.5 -STABLEpre2002-03-07, 4.5 -STABLE, -RELENG, 4.5 -RELEASE-p32, 4.5 -RELEASE, 4.5, 4.6 -STABLE, -RELENG, 4.6 -RELEASE-p20, 4.6 -RELEASE, 4.6, 4.6.2, 4.7 -STABLE, 4.7 -RELENG, 4.7 -RELEASE-p17, 4.7 -RELEASE, 4.7, 4.8 -RELENG, 4.8 -RELEASE-p7, 4.8 -PRERELEASE, 4.8, 4.9 -RELENG, 4.9 -PRERELEASE, 4.9, 4.10 -RELENG, 4.10 -RELEASE, 4.10, 4.11 -STABLE, 5.0 -RELENG, 5.0, 5.1 -RELENG, 5.1 -RELEASE-p5, 5.1 -RELEASE, 5.1, 5.2 -RELENG, 5.2 -RELEASE, 5.2, 5.2.1 -RELEASE, 5.3 -STABLE, 5.3 -RELEASE, 5.3, 5.4 -PRERELEASE; SuSE Linux 7.0, sparc, ppc, i386, alpha, 7.1, x86, sparc, ppc, alpha, 7.2, i386	nph-reg3rdpty1.pl/product=05529&platform=osx&method=sa/SecUpd2005-003Pan.dmg Debian: http://security.debian.org/pool/updates/main/n/netkit-telnet/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:01/ MIT Kerberos: http://web.mit.edu/kerberos/|advisories/2005-001-patch_1.4.txt Netkit: ftp://ftp.uk.linux.org/pub/linux/Networking/netkit/ Openwall: http://www.openwall.com/Owl/CHANGES-current.shtml RedHat: http://rhn.redhat.com/errata/RHSA-2005-327.html Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57755-1 SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/n/netkit-telnet/ OpenBSD: http://www.openbsd.org/errata.html#telnet Mandrake: http://www.mandrakesecure.net/en/ftp.php Gentoo: http://security.gentoo.org/glsa/glsa-200503-36.xml http://security.gentoo.org/glsa/glsa-200504-01.xml		US-CERT VU#341908 Gentoo Linux Security Advisory, GLSA 200504-04, April 6, 2005 SGI Security Advisory, 20050401-01-U, April 6, 2005 Sun(sm) Alert Notification, 57761, April 7, 2005 SCO Security Advisory, SCOSA-2005.21, April 8, 2005 Avaya Security Advisory, ASA-2005-088, April 27, 2005 Gentoo Linux Security Advisory, GLSA 200504-28, April 28, 2005 Turbolinux Security Advisory, TLSA-2005-52, April 28, 2005 Sun(sm) Alert Notification, 57761, April 29, 2005 **SCO Security Advisory, SCOSA-2005.23, May 17, 2005**

	Debian: http://security.debian.org/pool/updates/main/k/krb5/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-04.xml SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.21 Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57761-1 Openwall: http://www.openwall.com/Owl/CHANGES-current.shtml Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-088_RHSA-2005-330.pdf Gentoo: http://security.gentoo.org/glsa/glsa-200504-28.xml TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57761-1 OpenWall: http://www.openwall.com/Owl/CHANGES-current.shtml **SCO:** **ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2005.23** Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors Cisco Systems Cisco Aironet 1200 Series Access Point, 350 Series Access Point, Content Services Switch	A remote Denial of Service vulnerability has been reported in the Protection Against Wrapped Sequence Numbers (PAWS) technique that was included to increase overall TCP performance. Update information available at:	Cisco Various Products TCP Timestamp Denial of Service	Low	Cisco Security Notice, 64909, May 18, 2005 Microsoft Security Advisory (899480), May 18, 2005

11000 Series (WebNS), MGX 8200 Series Edge Concentrators, MGX 8800 Series Multiservice Switches, MGX 8900 Series Multiservice Switches, SN5400 Series Storage Routers; OpenBSD 3.x; Hitachi GR2000 Series Gigabit Routers, GR4000 Series Gigabit Routers, GS3000 Series Gigabit Switches, GS4000 Series Gigabit Switches; ALAXALA Networks AX5400S, AX7800R, AX7800S; FreeBSD FreeBSD 2.x, 3.x, 4.x	http://www.cisco.com/warp/public/707/cisco-sn-20050518-tcpts.shtml OpenBSD: ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.6/common/015_tcp.patch Hitachi: The vendor has issued updated versions. ALAXALA: Customers are advised to contact the vendor in regards to obtaining and applying the appropriate update. Microsoft: http://www.microsoft.com/technet/security/advisory/899480.mspx An exploit script has been published.	CAN-2005-0356		US-CERT VU#637934
Multiple Vendors Computer Associates BrightStor ARCServe Backup for Windows 11.1, eTrust Antivirus 6.0, 7.0, SP2, 7.1, eTrust Antivirus EE 6.0, 7.0, eTrust Antivirus for the Gateway 7.0, 7.1, eTrust Intrusion Detection 1.4.1 .13, 1.4.5, 1.5, 3.0, SP 1, eTrust Secure Content Manager 1.0, SP1, 1.1, InoculateIT 6.0, Vet Antivirus; Zone Labs ZoneAlarm Antivirus, ZoneAlarm Security Suite 5.1, 5.5.062.011, 5.5.062, 5.5	A heap overflow vulnerability was reported due to an integer overflow flaw in memory allocation and utilization routines when malicious compressed VBA projects are processed by the library, which could let a remote malicious user execute arbitrary code. Computer Associates: http://crm.my-etrust.com/CIDocument.asp?KDId=1588&GUID=CFCBAF561393476799582FB18E05F829 Currently we are not aware of any exploits for this vulnerability.	Computer Associates Remote Heap Overflow CAN-2005-1693	High	Security Focus, 13710, May 23, 2005 Computer Associates Vulnerability ID: 32896, May 24, 2005

Multiple Vendors
MPlayer 1.0pre6 & prior;
Xine 0.9.9-1.0;
Peachtree Linux release 1
	Several vulnerabilities have been reported: a buffer overflow vulnerability has been reported due to a boundary error when processing lines from RealMedia RTSP streams, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability has been reported due to a boundary error when processing stream IDs from Microsoft Media Services MMST streams, which could let a remote malicious user execute arbitrary code.
	Patches available at: http://www.mplayerhq.hu/MPlayer/patches/rtsp_fix_20050415.diff
		MPlayer RTSP & MMST Streams Buffer Overflow
		CAN-2005-1195
			High	Security Tracker Alert,1013771, April 20, 2005
				Gentoo Linux Security Advisory, GLSA 200504-19, April 20, 200
				Peachtree Linux Security Notice, PLSN-0003, April 21, 2005
				Xine Security Announcement, XSA-2004-8, April 21, 2005
				Gentoo Linux Security

	Gentoo: http://security.gentoo.org/glsa/glsa-200504-19.xml Patches available at: http://cvs.sourceforge.net/viewcvs.py/xine/xinelib/src/input/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-27.xml **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Slackware: ftp://ftp.slackware.com/pub/slackware/ Currently we are not aware of any exploits for these vulnerabilities.			Advisory, GLSA 200504-27, April 26, 2005 SUSE Security Summary Report, SUSE-SR:2005:012, April 29, 2005 Slackware Security Advisory, SSA:2005-121-02, May 3, 2005 **SUSE Security Summary Report, SUSE-SR:2005:013, May 18, 2005**
Multiple Vendors See US-CERT VU#222750 for complete list	Multiple vendor implementations of TCP/IP Internet Control Message Protocol (ICMP) do not adequately validate ICMP error messages, which could let a remote malicious user cause a Denial of Service. Cisco: http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml IBM: ftp://aix.software.ibm.com/aix/efixes/security/icmp_efix.tar.Z RedHat: http://rhn.redhat.com/errata/ Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57746-1 **ALAXALA: Customers are advised to contact the vendor in regards to obtaining and applying the appropriate update.** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendor TCP/IP Implementation ICMP Remote Denial of Service CAN-2004-1060 CAN-2004-0790 CAN-2004-0791	Low	US-CERT VU#222750 Sun(sm) Alert Notification, 57746, April 29, 2005 US-CERT VU#415294 **Security Focus, 13124, May 21, 2005**
NetWin SurgeMail 3.0 c2	Several Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary HTML and script code. A CVS fix is available from the vendor. There is no exploit code required.	NetWin SurgeMail Cross-Site Scripting CAN-2005-1714	High	Secunia Advisory, SA15425, May 19, 2005

Novell ZENworks Desktop Management 6.5, ZENworks for Desktops 3.2 SP2, 4.0, 4.0.1, ZENworks for Servers 3.2, ZENworks Remote Management Novell ZENworks Server Management 6.5	Several vulnerabilities were reported in the Remote Management authentication protocol in 'zenrem32.exe' due to integer overflows and boundary errors, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for these vulnerabilities.	Novell ZENworks Remote Management Buffer Overflows CAN-2005-1543	High	Securiteam, May 19, 2005
phpSysInfo phpSysInfo 2.3	Multiple Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code. It is also possible to obtain the full path to certain scripts. **Debian:** **http://security.debian.org/pool/updates/main/p/phpsysinfo/** There is no exploit code required; however, Proofs of Concept exploits have been published.	PHPSysInfo Multiple Cross-Site Scripting CAN-2005-0870	High	Secunia Advisory, SA14690, March 24, 2005 **Debian Security Advisory, DSA 724-1, May 18, 2005**
PortailPHP PortailPHP 1.3	An SQL injection vulnerability has been reported due to insufficient sanitization of user-supplied input before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept has been published.	PortailPHP ID Parameter SQL Injection CAN-2005-1701	High	Security Focus, 13708, May 23, 2005
PostNuke Development Team PostNuke Phoenix 0.750, 0.760 RC2 & RC3	Multiple vulnerabilities have been reported: a vulnerability was reported in 'index.php' due to insufficient sanitization of input passed to the 'module' and 'riga[0]' parameters before using in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a Cross-Site Scripting vulnerability was reported in 'index.php' due to insufficient verification of the 'skin' parameter before using in include files, which could let a remote malicious user include arbitrary files; a vulnerability was reported in 'demo.php' due to insufficient sanitization of the 'skin' and 'paletteid' parameters and in 'config.php' due to insufficient sanitization of the 'serverName' parameter, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability has been reported because it is possible to obtain the full path to certain scripts by	PostNuke Multiple Remote Input Validation CAN-2005-1694 CAN-2005-1695 CAN-2005-1696 CAN-2005-1697 CAN-2005-1698 CAN-2005-1699 CAN-2005-1700	High	PostNuke Security Advisory, PNSA 2005-2, May 20, 2005

	accessing them directly. Upgrades available at: http://news.postnuke.com/Downloads-index-req-viewdownloaddetails-lid-411.html http://news.postnuke.com/Downloads-index-req-viewdownloaddetails-lid-471.html There is no exploit code required; however, Proofs of Concept exploits have been published.			
PostNuke Development Team PostNuke Phoenix 0.760 RC3	Multiple vulnerabilities have been reported: Cross-Site Scripting vulnerabilities have been reported due to insufficient sanitization of the 'module' parameter in 'admin.php' and the 'op' parameter in 'user.php,' which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability has been reported due to insufficient sanitization of the 'sid' parameter before used in a SQL query, which could let a remote malicious user inject arbitrary SQL code. **Update information available at: http://news.postnuke.com/Article2691.html** Proofs of Concept exploits have been published.	PostNuke Phoenix Remote Cross-Site Scripting & SQL Injection CAN-2005-1048 CAN-2005-1049	High	Dcrab 's Security Advisory, April 8, 2005 **PostNuke Security Advisory, PNSA 2005-2, May 20, 2005**
S9Y Serendipity 0.8 -beta6 Snapshot, 0.8 -beta6, 0.8 -beta5, 0.8	Multiple vulnerabilities have been reported: a vulnerability was reported due to an error in the file upload handling, which could let a remote malicious user upload special files without privileges; and a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of input passed to the 'templatedropdown' and 'shoutbox' plugins, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://prdownloads.sourceforge.net/php-blog/serendipity-0.8.1.tar.gz?download There is no exploit code required.	Serendipity File Upload & Cross-Site Scripting CAN-2005-1712 CAN-2005-1713	High	Secunia Advisory, SA15405, May 18, 2005
Sun Microsystems, Inc. JavaMail 1.3, 1.3.2, Sun Solstice Internet Mail Server POP3 2.0	A vulnerability has been reported in the MimeMessage method in the Sun JavaMail API due to insufficient validation on message number values passed during requests, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Sun JavaMail API MimeMessage Information Disclosure CAN-2005-1682	Medium	Securiteam, May 19, 2005

ZyXEL Prestige 650R-31 3.40 KO.1	A remote Denial of Service vulnerability has been reported when handling specially crafted fragmented IP packets. No workaround or patch available at time of publishing. There is no exploit code required.	Zyxel Prestige 650R-31 Router Remote Denial of Service CAN-2005-1717	Low	Security Focus, 13703, May 20, 2005

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
May 24, 2005	haloloop.zip	No	Script that exploits the Gearbox Software Halo Game Server Remote Denial of Service vulnerability.
May 23, 2005	tcp_paws.c	Yes	Script that exploits the Multiple Vendor TCP Timestamp PAWS Remote Denial of Service vulnerability.
May 23, 2005	warkingsfs.zip wkbbugs.zip	No	Exploit scripts for the Warrior Kings And Warrior Kings: Battles Remote Format String & Denial of Service vulnerabilities.
May 22, 2005	picasm_exploit.c	Yes	Script that exploits the Picasm Error Handling Buffer Overflow vulnerability.
May 22, 2005	ecl-winipdos.c	No	Proof of Concept Denial of Service exploit for windows that takes advantage of an off-by-one validation error in the IP options field.
May 22, 2005	mfsa200539.txt	Yes	Proof of Concept exploit for the Mozilla Firefox sidebar code execution vulnerability.
May 17,2005	wartimesboom.zip	No	Proof of Concept exploit script for the War Times Remote Game Server Denial Of Service vulnerability.
May 17, 2005	fusion.php	No	Exploit for the Fusion SBX Authentication Bypass & Arbitrary Code Execution vulnerability.

[back to top]

Trends

- **Revenge is often the reason for computer sabotage, according to a new study by DHS:** According to a study paid for by the Department of Homeland Security, corporate insiders who sabotage computers so sensitive that they risk endangering national security or the economy commonly are motivated by revenge against their bosses. The study examined dozens of computer-sabotage cases over six years to determine what motivates trusted insiders to attack and how their actions damage the country's most sensitive networks and data. The review described most attackers as disgruntled workers or former employees--typically working in technology departments--who were angry over disciplinary actions, missed promotions, or layoffs. The attacks included deleting vital software or data, posting pornography on an employer's Web site, or crippling whole networks. Source: http://www.informationweek.com/story/showArticle.jhtml?articleID=163104819.

- **Lax security leaving networks wide open**: A newply published Harris poll has warned that lax firewall security is leaving companies open to the installation of malicious software on their internal networks. Fewer than half of companies block executable files from the internet, and the same percentage fail to prevent such software coming in via instant messaging. Some 40 per cent do not even block executables in email, the major cause of virus infections. Source: http://www.vnunet.com/vnunet/news/2135301/lax-security-leaving-networks-wide-open.
- **Underground showdown: Defacers take on phishers:** Groups fighting against online criminals intent on phishing have gained allies from another species of underground miscreant: Web-site defacers. A small percentage of Web sites illegally set up for phishing scams have been defaced with warnings to potential victims defacers. Source: http://www.securityfocus.com/news/11212.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Netsky-Q	Win32 Worm	Stable	March 2004
3	Mytob.C	Win32 Worm	Stable	March 2004
4	Zafi-D	Win32 Worm	Stable	December 2004
5	Netsky-D	Win32 Worm	Stable	March 2004
6	Lovgate.w	Win32 Worm	Stable	April 2004
7	Zafi-B	Win32 Worm	Stable	June 2004
7	Netsky-Z	Win32 Worm	Stable	April 2004
9	Netsky-B	Win32 Worm	Stable	February 2004
10	MyDoom-O	Win32 Worm	Stable	July 2004

Table Updated May 24, 2005

Viruses or Trojans Considered to be a High Level of Threat

- **Sober.Q**: German security experts claim to have stopped a new variant of the Sober virus, Sober.Q, which propagated right-wing hate messages in German and English. However, according to the German Federal Office for Information Security, Sober.Q is programmed to begin spreading its hate messages again on Thursday, May 26. Using a new list of Web sites, it could be the same story all over again. Source: http://www.ecommercetimes.com/story/security/43294.html

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Appdisabler.B	SymbOS/Appdisabler.B	Symbian OS Worm
Backdoor.Bifrose.C		Trojan
Del-476	Del-475 trj/killfiles.w trojan.win32.killfiles.hi	Trojan
Delf.fz	Trojan-PSW.Win32.Delf.fz	Trojan
Downloader-AAI		Trojan
Downloader-AAM		Trojan
Downloader-AAZ		Trojan
Downloader-ZL		Trojan
Druogna	Adware/BlueScreenWa TR/Agent.CT Trojan.Win32.Agent.ct Win32/Druogna.F!Trojan	Trojan
Gaobot.GLV	W32/Gaobot.GLV.worm	Win 32 Worm
Gorgs.A	Trj/Gorgs.A	Trojan
Oscarbot.F	W32/Oscarbot.F.worm	Win 32 Worm
PE_YAMI.A	Virus.Win32.Niya.a W32.Yami.A W32/NGVCK.d	Win 32 Worm
PWSteal.Bancos.V		Trojan
Small.avu	Backdoor.Win32.Dumadoor.bl Backdoor.Win32.Dumador.bl Downloader-ABC Trojan-Downloader.Win32.Small.avu W32/Small.avu	Trojan
Troj/Vidlo-J	Trojan-Downloader.Win32.Vidlo.m Downloader-AAP	Trojan
Troj/Zapchas-J	Backdoor.Win32.mIRC-based Backdoor.IRC.Zapchast IRC/Flood.mirc	Trojan
TROJ_PGPCODER.A	PGPcoder Trojan.Pgpcoder Virus.Win32.Gpcode.b	Trojan

TROJ_PGPCODER.A	PGPcoder Trojan.Pgpcoder Virus.Win32.Gpcode.b	Trojan
TROJ_VIPERIK.A		Trojan
Trojan.Dazheb		Trojan
Trojan.Webloin		Trojan
Trojan.Webus.F		Trojan
W32.Kelvir.CG		Win 32 Worm
W32.Lanieca.B@mm		Win 32 Worm
W32.Linkbot.M	Backdoor.Win32.PoeBot.b W32/Poebot.gen	Win 32 Worm
W32.Mytob.CP@mm	Net-Worm.Win32.Mytob.x W32/Mytob-AN	Win 32 Worm
W32.Mytob.CQ@mm	Net-Worm.Win32.Mytob.x W32/Mytob-AM W32/Mytob.gen@MM WORM_MYTOB.EX	Win 32 Worm
W32.Picrate.C@mm		Win 32 Worm
W32.Stubbot.A@mm		Win 32 Worm
W32/Agobot-AAZ		Win 32 Worm
W32/Alcra-A	WORM_ALCAN.A W32.Alcra.A W32/Alcan.worm!p2p P2P-Worm.Win32.Alcan.a W32.Alcra.A	Win 32 Worm
W32/Eyeveg.worm	Backdoor-AYU Backdoor.Lorac BKDR_LORRAC.A Troj/Eyeveg-A W32.Lorac W32/Lorac.A Win32/Atak.Variant!Worm Worm.Win32.Eyeveg Worm.Win32.Eyeveg.a WORM_WURMARK.M	Win 32 Worm
W32/Farack!p2p		Win 32 Worm
W32/Kassbot-D	Backdoor.Win32.Delf.zq	Win 32 Worm
W32/Kelvir.worm.bh		Win 32 Worm
W32/LastFour.ow		Win 32 Worm
W32/Mytob-AM	Net-Worm.Win32.Mytob.x W32/Mytob.gen@MM	Win 32 Worm
W32/Mytob-AN	Net-Worm.Win32.Mytob.x	Win 32 Worm
W32/Mytob-CK	WORM_MYTOB.DQ W32.Mytob.R@mm Net-Worm.Win32.Mytob.w	Win 32 Worm
W32/Mytob-CL	Net-Worm.Win32.Mytob.x	Win 32 Worm
W32/Mytob-EM	WORM_MYTOB.EM Net-Worm.Win32.Mytob.t W32.Mytob.CF@mm	Win 32 Worm

W32/Mytob-I	Net-Worm.Win32.Mytob.gen W32/Mytob.gen@MM	Win 32 Worm
W32/Opanki-I	IM-Worm.Win32.Opanki.b WORM_OPANKI.I	Win 32 Worm
W32/Oscabot-F	TROJ_DLOADER.LS	Win 32 Worm
W32/Qeds-A	Trojan.Win32.VB.xb W32/Qeds	Win 32 Worm
W32/Rbot-ADA	W32/Sdbot.worm.gen WORM_RBOT.AZM	Win 32 Worm
W32/Rizon-B	Trojan.Win32.VB.uj W32/Rizon.worm	Win 32 Worm
W32/Sdbot-YJ	Backdoor.Win32.Rbot.gen W32/Sdbot.worm.gen.w W32.Spybot.Worm WORM_SDBOT.BVC	Win 32 Worm
W32/Sober.q!spam		Win 32 Worm
Win32.Alcan.A		Win 32 Worm
Win32.Angourd Family		Win 32 Worm
Win32.Druogna Family		Win 32 Worm
Win32.Helmut.A		Win 32 Worm
Win32.Maddle Family		Win 32 Worm
Win32.Mytob.CX		Win 32 Worm
Win32.Mytob.CZ		Win 32 Worm
Win32.NerdBot Family		Win 32 Worm
Win32.Rbot.CMG		Win 32 Worm
Win32.SillyDl.NT		Win 32 Worm
Win32.Sonebot.A		Win 32 Worm
Win32.Trykid Family		Win 32 Worm
WORM_COMBRA.C	W32/Combra.worm	Win 32 Worm
WORM_KIBUV.B	Backdoor.StdBot.a Bloodhound.Exploit.8 Exploit-MS04-011.gen W32.Shelp W32/Stdbot.worm Win32.Kibuv.B	Win 32 Worm
WORM_MYTOB.EU	W32/Mytob Net-Worm.Win32.Mytob.j W32.Mytob.CM@mm	Win 32 Worm
WORM_OPANKI.P	W32/Opanki	Win 32 Worm
Wurmark.L	Email-Worm.Win32.Wurmark.l	Win 32 Worm

[back to top]

Last updated May 25, 2005